DOCUMENT RESUME

ED 163 914 IR 006 386

AUTHOR	Ware, Willis H.
TITLE	Computer Technology: For Better or Worse?
INSTITUTION	Rand Corp., Santa Monica, Calif.
REPORT NO	P-5903
PUB DATE	Jul 77
NOTE	11p.; Paper presented at the National Bureau of Standards Conference on Trends in Applications 1977: Computer Security and Integrity (Washington, D.C., May 19, 1977); For related document, see IR 006 385
AVAILABLE FROM	Publications Department, The Rand Corporation, 1700 Main Street, Santa Monica, Calif. 90406 ($1.50)
EDRS PRICE	MF-$0.83 HC-$1.67 Plus Postage.
DESCRIPTORS	Civil Liberties; Confidentiality; *Electronic Data Processing; *Futures (of Society); Government Role; *Information Dissemination; Information Processing; *Privacy; Public Policy

ABSTRACT

Computer technology ought to be among the most helpful and useful of any technology, but if it is not treated with care, the society will be worse off for it. The Federal Privacy Act of 1974 established the Privacy Protection Study Commission whose business started in June, 1975. In examination of the private sector, the commission's recommendations reflected three broad principles: (1) recordkeeping practices should minimize intrusiveness of collection to the individual, (2) recordkeeping practices should maximize the fairness with which decisions about people are made, and (3) there should be legitimate and enforceable expectation of confidentiality with respect to the records that are maintained about an individual. Implementation of the Privacy Act can be accomplished by amending existing laws (notably the Federal Credit Reporting Act) and by enactment of new legislation. To implement security precautions in responding to privacy, it is important to utilize good information management practices with tight controls on the use of information. Future systems will need to control access at the "data element" level to insure privacy in exchange of records among automated recordkeeping systems. Discussion is based on recordkeeping practices in the areas of credit granting, depository, education, medical, insurance, research and statistics, investigatory, employment, tax records, and mailing lists. (JEG)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

ED163914

I R

U.S. DEPARTMENT OF HEALTH,
EDUCATION & WELFARE
NATIONAL INSTITUTE OF
EDUCATION

THIS DOCUMENT HAS BEEN REPRODUCED EXACTLY AS RECEIVED FROM THE PERSON OR ORGANIZATION ORIGINATING IT. POINTS OF VIEW OR OPINIONS STATED DO NOT NECESSARILY REPRESENT OFFICIAL NATIONAL INSTITUTE OF EDUCATION POSITION OR POLICY

COMPUTER TECHNOLOGY: FOR BETTER OR WORSE?

"PERMISSION TO REPRODUCE THIS MATERIAL HAS BEEN GRANTED BY

Rand Corp.

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC) AND USERS OF THE ERIC SYSTEM."

Willis H. Ware

July 1977

IR000 386

P-5903

COMPUTER TECHNOLOGY: FOR BETTER OR WORSE? *

The question posed in the title is of obvious importance to each of us as computer professionals and to the country. Will we regret ever having conceived the computer or will it prove an indispensable and properly controlled technology? The answer to it: yes, computer technology ought to be among the most helpful and useful of any technology; if it is not treated with care, the answer will be no, society will be worse off for it.

We have all had experience with computer systems that treat us unkindly, systems that send bills but do not tell us the due date, but instead tell us in how many days it is due. We all know systems in which it is almost impossible to find a human being with which to deal in correcting an error--systems that evidently have been designed with little thought for the individuals that are to be served. By now, there is even a phrase to describe them--inhumane systems. Sometimes an inhumane system is because the management that commissioned it does not understand the niceties of a courteous computer system; perhaps it does not budget well enough or it does not write the requirements properly. Perhaps the management does not understand that when moving from a paper oriented system to a computer oriented system, some things are unavoidably different. Sometimes the management abdicates its responsibilities and turns to its computer specialists, saying: "produce a system." When that happens, we do design and produce a system from our perspective of the requirement, not from the perspective of what management really ought to be asking for.

In that regard, it is easy to be critical of our profession and to say the kind thing that we are sometimes inconsiderate, sometimes naive, sometimes thoughtless, sometimes narrowsighted, and sometimes insensitive to societal needs. It is also easy to say cruelly that we are professionally arrogant, driven by our own sense of technical superiority to design the tight system that does its function with a minimum amount of equipment and expense, and operates as though the environment always will behave benignly but never misbehave capriciously. Even worse, we can be accused of designing a system that views the individual to be served as just another parameter

---

* This keynote speech was presented at the National Bureau of Standards Conference on "Trends in Applications 1977: Computer Security and Integrity," sponsored by NBS, the IEEE Computer Society and the IEEE; Washington, D.C.; May 19, 1977.

of the work load, not as a human being that deserves to be treated in a friendly, forgiving, and foolproof courteous fashion.

The circumstance of the inhumane system is one of our own making, perhaps shared with an irresponsible or abdicating management. The area I want to concentrate on is one in which we will not have a choice--an area in which information management principles will be specified as law and it will be our obligation to respond. The area is privacy. You are undoubtedly aware of the Federal Privacy Act of 1974, and you may be aware of the operational behavior that it imposes on Federal agencies. It also gives to each of us as a citizen certain rights to see records about oneself, to challenge the content of the record, and to cause errors to be corrected. It is an omnibus law that throws a broad pattern of behavior across all Federal agencies and requires each of them to respond to the same set of requirements and goals.

I note in passing that as the country struggles to bring the interface between its citizens and all the recordkeeping systems that surround us into proper balance, we have ahead a very difficult and a very complex situation to solve. I make the observation because it has become quite clear to the Commission as a result of an examination of the compliance of Federal agencies with the Act that not all bad practices have been remedied and not all socially undesirable consequences have been eliminated. While the Act has taken a very important initial step, any pragmatic person would never have expected it to solve all aspects of the problem at the beginning because of the intricate nature of the situation. It has taken an important and significant first step in an appropriate direction; my judgment is that in the next year or two, the country will take the second step.

Among other things, the Act established the Privacy Protection Study Commission whose business started in June of 1975 and is presently scheduled to conclude on 30 September 1977. The final report is anticipated in mid-July with several supplementary volumes thereafter. At the top of our priority list has been an examination of the private sector, its recordkeeping practices, present or potential abuses and appropriate remedial actions.

You will remember the history of privacy, although it has not always been identified as such at the time certain important legislative actions

were taken. In one way or another, the Fair Credit Reporting Act, the Fair Credit Billing Act, the Family Educational Rights Act, the Equal Opportunity Employment and Equal Opportunity Credit Acts all deal with the interface between individuals and records. Clearly, the Commission has been influenced by such a heritage and by the details of the laws that have been passed. However, in contrast to the omnibus nature of the Privacy Act for the Federal sector, we have consciously decided that an omnibus statute is inappropriate for the private sector. The basis for the position is the observation that relative to the Federal government, the private sector is a large, diverse and complex environment. The recordkeeping practices vary widely from industry to industry; the opportunities for misuse of records vary widely; and the organizational and managerial motivations are quite different from a bureaucracy. It seemed to us that there could be no single set of recommendations framed to cover such a broad, diverse environment of problems. Therefore, our recommendations will call for implementation in a variety of fashions. Sometimes we will ask for amendments of existing law, notably the Federal Credit Reporting Act; occasionally we will ask for the enactment of some new legislation; occasionally we will suggest that compliance be through existing regulatory mechanisms at state level.

In our examination of the private sector, we have looked at recordkeeping practices of a large number of areas: credit granting, depository, education, medical, insurance, research and statistics, investigatory, employment, tax records and mailing lists. Notable by its exception is law enforcement and criminal processes, an important area that we did not have an opportunity to examine--and it obviously needs attention. Our recommendations and implementation strategy are keyed to areas; and in addition, we will also report an assessment of the compliance of Federal agencies with the 1974 Privacy Act. Of necessity, we will take a position on the Social Security Number and its role in recordkeeping.

You will remember that the report of the Secretary's Advisory Committee on Automated Personal Data Systems built its argument on five principles.*

---

*"Records, Computers and the Rights of Citizens," Datamation, September 1973. A review of "Records, Computers and the Rights of Citizen," Report of the Secretary's Advisory Committee on Automated Personal Data Systems, chaired by W. H. Ware, Department of Health, Education and Welfare, July 1973, DHEW Publication No. (OS)73-97. Available through the U.S. Government Printing Office, Stock Number 1700-00116.

In paraphrase they are: no secret record system should exist, a citizen has the right to see his record, a citizen has the right to cause an error to be corrected, a citizen should be able to prevent information collected for one purpose from being used for others without his consent and organizations should exhibit responsible recordkeeping practices. We have generalized and extended the conceptual framework. Our recommendations will be cast in terms of three broad principles. The social expectation is that:

1. Recordkeeping practices should minimize intrusiveness of collection to the individual;
2. Recordkeeping practices should maximize the fairness with which decisions about people are made; and
3. There should be a legitimate and enforceable expectation of confidentiality with respect to the records that are maintained about an individual.

While the HEW principles addressed recordkeeping practices and rights of the individual rather directly, the three of the Commission are geared to broad social expectations in behalf of the individual. Our recommendations follow the principles.

It would be inappropriate and needless to examine each recommendation in turn, but I would like to give the general thrust of them by noting a few typical ones. First, when an adverse decision is made about an individual on the basis of information in a record, the individual should be told exactly what items in the record are the basis for the adverse decision. Secondly, in contrast to the language of the Fair Credit Reporting Act which provides that an individual should be told about the contents of his record, we will recommend in every area that the individual should have a broad right to see his record in a form comprehensible to him and to copy it. An obvious exception that we have to allow is cases where there is a reasonable expectation of fraud or other illegal activity. Next, the individual should have a broad right to cause errors to be corrected and to have those corrections forwarded to organizations that have already received erroneous information; and in some cases, to also cause corrections to be passed backward to data sources.

Organizations that collect information from people should clearly tell the individual why it is being collected, how it will be used, with whom it will be shared, how it might be verified, and what other organizations might be contacted to supplement it. In effect, we are asking organizations in the private sector to be fully open when they seek to collect information from an individual. Next, any form that an individual signs to authorize access to other sources of information about him should be specific about the organization to be approached, specific to purpose, specific in scope, dated and of specified calendar duration. Information should not be collected from people by pretext methods. If one wishes information from an individual, be open and forthright about why. Certain techniques of information collection should, because of intrusiveness, be prohibited in certain areas--a notable example is the polygraph. An individual should be notified by a recordkeeper before the recordkeeper responds to a subpoena or other compulsory process, so that the individual may have an opportunity to squash the subpoena or defend himself. Again, there is an obvious exception that has to be made for an investigation relative to suspected crime. Next, there should exist mechanisms within government whereby individuals can bring to the attention of government instances of intrusive collection or collection of facts for certain purposes. An example of government response is California's prohibition against use of life style information and sexual preferences for insurance decisions. In certain areas--notably social service and social assistance areas--disclosures of personal information may not be made without the consent of the individual, unless the disclosures are mandated by law. In the same area, an individual should have the right to insist that any contacts made to verify information that he has provided be conducted in such a way that the nature of the service applied for not be revealed.

The ones that I have mentioned are illustrative and phrased in a very general way. You will expect in our written report to find the language more precise and to find recommendations detailed area by area. All in all, I suspect that we have formulated about 150 recommendations spread over a dozen or so areas that we have examined. There are, of course, similarities from area to area.

What does it all mean to each of us as a computer professional? What does it mean to the computerized record system? I'd like to share with you some thoughts that are by no means complete, but hopefully I can highlight some important consequences. First I'd make a comment about the role of the technologist in the whole privacy matter. By its nature, legislation is general; it establishes broad social policy and goals. While it sometimes includes hard numbers, such as emission standards or speed limits, for the most part legislation speaks broadly. The problem then becomes how to detail and interpret broad policy; in our system of government, it comes from case law developed by the courts and from administrative rulings of government bodies. Thus, as you read our recommendations, you will find them liberally sprinkled with what would seem to be "weasel words." There will be phrases like "reasonable effort," or "reasonable procedure," or "appropriate safeguards;" but the point is that phraseology of such kind is essential in legislation. One does not wish to specify details so precisely that technological progress end runs the intent of the law. While Congress and other legislative bodies obviously must be attentive to the specifics of technology and its progress, it would be inappropriate for such a body to prepare legislation which said in ultimate detail: "this is the way it must be done." Any one of us will feel in a very uncomfortable position because each one in technology is trained and accustomed to work from very detailed specifications of a problem and to find a solution for its specifications. We tend to find ourselves frustrated by laws that regulate information useage and management; we characterize them categorically as too vague and claim that we do not know how to respond. Regrettably, we will have to respond.

In the private sector, it seems to me that the onus will fall on corporate management to make a judgment as to what privacy law means. It will be a long time before case law builds up and it will be a long time before preferred industry practices evolve. Therefore, the first few years of responding to new laws may be very exciting, if not unnerving, as managements struggle to decide whether their information practices and recordkeeping practices conform with the perceived intent of the law. Our role is to assist management in arriving at that position. Ultimately, computer people will have to decide what safeguards to put in place; we will have to decide what recordkeeping processes will have to be implemented and how. First, though we have a very essential role of aggressively helping management converge

to an appropriate posture. While there cannot be a dialogue between us and legislators, there can be, and I will argue vigorously that there must be, a dialogue between us as technologists and our managements in order that compliance with privacy law gets launched properly. The technologist understands his art but it is much easier for him to move into the area of the legislator--to understand such things as judicial procedure, due process, and legislative history--than for the legislative professional to move into our area and understand the intimate details and implications of technical matters.

I urge that each of us as a responsible technologist in his field extend himself toward the policymaker, to understand the intent and thrust of privacy law but not ask him to supply fine-grain details. On the other hand, I would say to management that you must not abdicate your responsibility to make necessary decisions and set appropriate policy. You must not say to your computer establishment: "Solve my problem; take care of privacy for me." By way of reminding you to take part in this dialogue, I would caution both sides that the Federal act now does and future law will also include civil and criminal sanctions for misbehavior. So take care. I stress the point one other way. Our recommendations establish for the individual an expectation that records about him will be treated in confidence; thus, the individual will acquire what the lawyer calls an assertable interest in law that can be defended in court. The net effect is to give each individual an assertable interest in your professional affairs as well, and in your technological performance.

Since this is a conference on security, I want to touch briefly on it; I need not remind you of a definition. Since privacy concerns itself with proper use of information, obviously security is an essential ingredient to any response to privacy. Based on our observation of compliance of Federal agencies with the existing Act, we would conclude that the prevailing concept of security vis-a-vis privacy is inappropriate. Privacy concerns itself with the fair use of information; thus, the trouble is likely to be the actions of authorized recipients of information and not the deliberate penetrator who pirates information. It is not the deliberate penetrator that is the security risk to privacy; rather, it is the behavior of the individuals authorized to have information--all of whom may be totally honest--that become the concern in privacy affairs. We have found the response of

Federal Agencies frequently has been against the threat of the deliberate penetrator. There has been a misplaced emphasis with regard to security; and in many cases, there has been technological overkill. Thus, the point of view of security is somewhat different when privacy, rather than national defense is the concern. To implement security precautions in responding to privacy, the first thing to be done--perhaps the most important thing--is simply to implement good information management practices. There will have to be tight management controls on the use of information; there will have to be extensive audit trails so it can be ascertained who has received what. There will have to be comprehensive corporate policy so that honest authorized users of the system know within what bounds each must function.

There will have to be comprehensive management oversight of the system and obviously there will have to be disciplinary actions established by corporate policy to remind people not to deal inappropriately with information from the system. When privacy is the concern to security, it is not bad people doing wrong things; it is good people, who may be totally honest, inadvertently or unknowingly doing wrong things. Provable security kernels and loopholes or trapdoors in an operating system take second place in importance.

There are technical consequences--in fact quite a few of them; but I will single out what appear at the moment to be the three most important. It is easiest to do by example. The thrust of modern technology is to break down the traditional barriers between organizational groups and their record-keeping systems; it also permits recordkeeping of a kind not possible with a paper system, the obvious example being any nationwide system. Consider the hospital medical record. Typically, it contains the following kinds of information: directory information (name, address, phone number, room number); medical treatment of which about a third will have come from a physician; drug prescriptions; special services such as X-rays or crutches; financial information on the patient; and most assuredly, his insurance circumstances. In modern record systems, it will be all in one big record. In our current society, medical records are shared with non-medical institutions for a variety of purposes: credit bureaus, insurance, third party payors, investigatory agencies and sometimes employment agencies. It is unlikely that anyone has need of the entire content. It is clear that even within the hospital there is a question of who is entitled to see what. Directory information

presumably is available to anyone; medical treatment information is presumably restricted to physicians and health care providers. On the other hand, drug treatment information is important, not only to the physician, but also to the pharmacy and also the accounting department; special services are also of interest to both the physician and to accounting. Presumably insurance information is of interest to accounting and perhaps to credit grantors.

In today's state of the art, when one speaks of "access to a record" it is commonly understood to mean the whole thing. It will have to change. It is clear that future systems will have to control access at lower than record level; it may even be necessary to control access at the data-element level. There is a granularity issue that is technical in nature and that will characterize future recordkeeping systems.

To respond to the problem and do such a fine-grain access control, the record has to contain "descriptor data" or a "descriptor feature" in order to assist the access control mechanism in providing the right portions of the record to the right recipient. Finally, a third technical consequence extends from our recommendations that stipulate propagation of error correction sometimes forward and sometimes backward. The record will have to contain information about sources of facts and about recipients; one might call it "traffic flow data." Since not all recipients will have received all parts of the record, there is a granularity problem with the traffic flow data as well. The three technical aspects obviously will be reflected in intricate software and file structures different than we now have. Each stems quite directly from privacy legislation as it collides with the forward thrust of computer technology.

As a final note, since the future is one of exchange of records among automated recordkeeping systems, the participating parties in any exchange will have to be aware of the presence and details of such supplementary information--descriptor and traffic flow data. There are other technical implications, but probably not as compelling nor as dominant technically as the ones just suggested.

There you have an overview of the privacy issue. It represents a significant amount of work ahead for all of us, but I say to you and I say to myself: "I wish us well as we approach it." I also say that it will be worth the effort everyone will make because as a country supported by a critical technology, we are about to make an enormous advance in the fairness with which recordkeeping systems treat people.